



1-31-06

AF\$
2/1/06

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **E. M. Hamann, et al**

Express Mail: EQ 088973145 US

Date: January 30, 2006

Serial No.: **09/492,632**

Filed: **January 27, 2000**

Docket No.: **GE998-005**

COMMISSIONER FOR PATENTS
Alexandria, VA 22313-1450

Sir:

Transmitted herewith is an **Appeal Brief** in the above-identified Application.

The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to **Deposit Account No. 50-0510**. A **duplicate copy** of this sheet is enclosed.

- X \$500.00 for filing a brief in support of an appeal in accordance with 37 CFR 41.20(b)(2).
- X Any additional filing fees required under 37 CFR \$1.16.
- X Any patent application processing fee under 37 CFR \$1.17.

02/01/2006 HTECKLU1 00000056 500510 09492632

01 FC:1402 500.00 DA

Respectfully submitted,
E. Hamann, et al

Anne Vachon Dougherty
Anne Vachon Dougherty
Registration No. 30,394
Tel. (914) 962-5910



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS
BEING DEPOSITED WITH THE UNITED STATES POSTAL
SERVICE AS EXPRESS MAIL IN AN ENVELOPE ADDRESSED TO:
COMMISSIONER FOR PATENTS, BOARD OF PATENT APPEALS,
P.O. BOX 1450, ALEXANDRIA, VIRGINIA 22313-1450, ON
DATE OF DEPOSIT: January 30, 2006
EXPRESS MAIL CERTIFICATE NO: E0088973145US
PERSON MAKING DEPOSIT: ANNE VACHON DOUGHERTY

Anne Vachon Dougherty 1/30/06
Signature & Date

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of	:	January 30, 2006
E.M. Hamann, et al	:	Group Art No.: 2131
Serial No. 09/492,632	:	Examiner: Syed Zia
Filed: January 27, 2000	:	for IBM Corporation Anne Vachon Dougherty 3173 Cedar Road Yorktown Hts, NY 10598
Title: DIGITAL SIGNATURE	:	

Board of Patent Appeals and Interferences
Washington, D.C. 20231

APPEAL BRIEF (37 CFR 41.37)

Appellants hereby appeal to the Board of Patent Appeals and Interferences from the decision dated July 7, 2005 of the Primary Examiner finally rejecting Claims 1-11 and 13 in the above-identified patent application, and respectfully

request that the Board of Patent Appeals and Interferences consider the arguments presented herein and reverse the Examiner's rejection.

I. REAL PARTY IN INTEREST

The appeal is made on behalf of Appellants who are real parties in interest with respect to the subject patent application.

II. RELATED APPEALS AND INTERFERENCES

There are no pending related appeals or interferences with respect to the subject patent application.

III. STATUS OF CLAIMS

There are twelve (12) claims pending in the subject patent application, numbered 1-11 and 13. No claims stand allowed.

A complete copy of the claims involved in the appeal is attached hereto.

IV. STATUS OF AMENDMENTS

There are no unentered amendments filed subsequent to final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The subject invention comprises apparatus, a method, and a program storage device for generating a digital signature. Claims 9-10 are directed to a signature device (Figs. 1, 2 and 7); Claims 1-8 and 13 are directed to a method for generating a digital signature (Figs. 3 and 5); and, Claim 11 is directed to a program storage device readable by machine tangibly embodying a program of instructions executable by the machine for performing the method for generating a digital signature.

The signature device, such as a chipcard (101 of Figs. 1 and 2), includes a signature program and additional signature certificate information (201) for providing an expanded electronic signature to sign a document (page 6, lines 16-22). The signature device executes the signature

program and does not require that an external authenticating entity generate the digital signature when the user is attempting to digitally sign a document ("the external and internal information together with the hash are merged on the chipcard 101", from page 13, line 14; "merger is effected by the chipcard program", from page 13, line 18; and, "[t]his encryption takes place on the chipcard", from page 14, lines 11-12). The digital signature (Fig. 7) includes an identifier of the signature device as well as at least one identifying characteristic (Chipcard Program ID of Fig. 7) indicating the hardware and software environment used in generating the electronic signature (see: page 3, lines 1-3; page 4, lines 1-4; page 13, lines 4-7; and page 15, lines 6-9) as well as a document extract value (Document ID of Fig. 7) identifying the document which is being signed (see: page 12, lines 19-20; and page 14, lines 23-24).

All of the independent claims, Claims 1, 9, 11, and 12 as amended, expressly recite that the signature device stores the signature program which is to be executed as well the necessary additional information so that it can perform digital signing of a document, and that the digital signing incorporates an identifier of the signature device as well

as at least one characteristic indicating the hardware and software environment used in generating the signature, as well as a document extract value for the document to be signed.

VI. GROUNDS OF REJECTION TO BE REVIEWED

The issue on appeal is whether the Examiner erred in rejecting Claims 1-11 and 13 as anticipated by U. S. Patent 6,662,151 of Schaefer-Lorinser (hereinafter "the Schaefer-Lorinser patent").

VIII. ARGUMENT

Appellants believe that the Examiner erred in rejecting the pending claims as anticipated by the teachings of U.S. patent 6,662,151 of Schaefer-Lorinser.

Independent Claims 1, 9 and 11

The Schaefer-Lorinser patent is directed to a system for secured reading and processing of data on intelligent data carriers, even when the terminal which is reading and processing the data is not connected to a server for authentication of the data carrier. Under the Schaefer-Lorinser system and method, the data carrier (i.e., the chipcard) and the terminal exchange cryptograms for authentication of the data carrier. Data used for generating a cryptogram at the data carrier is encoded at the data carrier when it is first issued (see: Col. 3, lines 51-55). Similarly, data used for generating cryptograms at the terminal is permanently stored at the terminal (see: Col. 4, lines 6-8), so that connection to a server is not required for authentication. As taught by Schaefer-Lorinser at Col. 3, lines 52-56, the data carrier/chipcard has a certificate "representing an electronic signature". When the data carrier generates a so-called "acknowledgment cryptogram" (Col. 4, lines 61-64) that is the electronic signature, e_3 , (see, Fig. 2) the data carrier applies a signature function, S_{card} , (defined at Col. 3, lines 65) on a data set comprising the ID number of the data carrier, a

posting data record, Db, (see: Col. 4, lines 54-55) and a random number, R3, which has been generated by the terminal (se: Col. 4, lines 47-48).

Appellants respectfully assert that the Schaefer-Lorinser patent does not teach or suggest the invention as set forth in independent Claims 1, 9 and 11. Appellants believe that the Schaefer-Lorinser does not teach or suggest the steps and means for performing the steps of executing the signature program including the claimed creating and encrypting. The present invention first creates a signature data set which comprises the received input information, an identifier to identify the signature device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature, and a document extract value.

Schaefer-Lorinser does not teach or suggest the existence or use of an identifying characteristic of the hardware and software environment used for generating the digital signature. Such is clearly taught by the present Specification, for example on page 13, lines 1-12, to include, in addition to an identifier, a signature counter value, an indication of the encryption method used, or an

identifier of the program such as a license number or program serial number, and is now expressly claimed. Furthermore, the Schaefer-Lorinser use of a "posting data record" is not the same as or suggestive of a document extract value of a document for signing, as is taught and claimed for the present invention. Schaefer-Lorinser's posting data record records the currency and amount of the debit and the posting number and time. Such information is not a document extract value.

It is well established under U. S. Patent Law that a prior art reference anticipates the claimed language under 35 USC 102 only if every element of the claimed invention is identically shown in that single reference, arranged as they are in the claims (*In re Bond*, 910 F. 2d 831, 832, 15 U.S.P.Q. 2d 1566, 1567 (Fed. Cir. 1990)). Since the Schaefer-Lorinser patent does not teach the signature device and method as claimed, including means and steps for a signature device, having a signature program and certificate, to generate a digital signature which identifies the signature device and at least one characteristic of the environment used to generate the signature, and uses a document extract value for the

document to be signed, it cannot be maintained that the Schaefer-Lorinser patent anticipates the invention as set forth in the independent claims, Claims 1, 9 and 11.

Claims 2 and 3

Claims 2 and 3 include all of the limitations of Claim 1, from which they depend, and further recite procuring the value of a signature counter from the signature device (Claim 2) and crating a signature counter as an attribute of the signature key prior to said procuring (Claim 3). Appellants rely on the arguments set forth above with regard to the claim limitations found in the independent claim. Appellants further contend that the teachings cited against Claim 2, from Col. 4, lines 17-23, provide no mention of a signature counter. Clearly, therefore, the cited teachings do not anticipate the language of Claim 2, and of Claim 3 which depends therefrom.

Appellants note that the teachings from Col. 4, lines 23-65, cited against Claim 3, also do not mention a counter as an attribute of a signature key. The mention of a chipcard posting sequence number (i.e., debit record) is not

the same as having a signature counter as an attribute of a signature key. Moreover, the Schaefer-Lorinser posting sequence number is noted as part of its D value (see: Col. 4, lines 55-58) and not as an attribute of a signature key.

Claim 4

Claim 4 includes all of the limitations of Claim 1, from which it depends, and further recites procuring the identifying characteristic from the signature device. Appellants rely on the arguments set forth above with regard to the claim limitations found in the independent claim. With regard to the further limitations recited in Claim 4, the Examiner has cited the passage from Col. 4, lines 36-51. The actions described therein, decrypting a cryptogram, are exclusively performed at the terminal, which clearly cannot anticipate a receiving step at the signature device.

Claim 5

Claim 5 includes all of the limitations of Claim 1, from which it depends, and further recites procuring information as to the hardware and software environment used

in creating the digital signature. Appellants rely on the arguments set forth above with regard to the claim limitations found in the independent claim. With regard to the further limitations recited in Claim 5, the cited Schaefer-Lorinser passage from Col. 3, lines 23-32 discusses that, for "electronic purse" applications, a terminal is not connected to a server. The passage does not, however, make any mention of a terminal procuring information about the hardware and software environment used to create a digital signature.

Claims 6, 7 and 8

Claim 6, and Claims 7 and 8 which depend therefrom, include all of the limitations of Claim 1, from which they directly or indirectly depend, and further additional limitations. Appellants rely on the arguments set forth above with regard to the claim limitations found in the independent claim. With regard to the further limitations recited in Claim 6, wherein the method further comprises entering an identifying characteristic to identify a holder of the signature key prior to receiving input information, the cited passage from Col. 4, lines 23-45 does not make any

mention of a holder of a signature key, let alone of entering an identifying characteristic to identify a holder prior to receiving input information (Claim 6), of crating the identifying characteristic as an attribute of the signature key (Claim 7), or of changing the identifying characteristic (Claim 8). The cited passage describes generating a random number and a cryptogram which includes the amount of money stored on the chipcard. Neither the random number nor the cryptogram comprises an identifying characteristic identifying the holder of the signature key. Clearly, therefore, the cited passage does not anticipate the invention as claimed.

Claim 13

Claim 13 includes all of the limitations of Claim 1, from which it depends, and further recites that the identifying characteristic comprises information which uniquely identifies the digital signature in relation to every other digital signature generated with the same signature key. Appellants rely on the arguments set forth above with regard to the claim limitations found in the independent claim. With regard to the further limitations

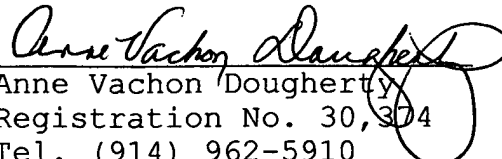
recited in Claim 13, the cited passage from Col. 4, lines 45-51 makes no mention of any other digital signatures, let alone of including an indication thereof in a signature data set.

CONCLUSION

Appellants respectfully assert that the Examiner has erred in rejecting all of the pending claims under 35 USC 102(e) as anticipated by the Schaefer-Lorinser patent. Appellants request that the decision of the Examiner, rejecting all of the pending claims, be overturned by the Board and that the claims be passed to issuance.

Respectfully submitted,
E. Hamann, et al

By:


Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910

VIII. CLAIMS APPENDIX

1. A method for generating a digital signature in a signature device having a signature program and certificate with signature key stored thereon for the signing of a document, wherein the digital signature identifies said device and at least one characteristic of the hardware and software environment used for generating said digital signature in said signature device, comprising the steps of:
 - a) receiving input information to said signature device; and
 - b) executing said signature program by the steps of: creating a signature data set comprising at least the received information, an identifier to identify said signature device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature, and a document extract value of the document for signing; and

creating an expanded digital signature by encrypting the signature data set with the aid of a signature key stored in said certificate.

2. The method in accordance with Claim 1, wherein said receiving input information comprises procuring the value of a signature counter from said signature device.
3. The method in accordance with Claim 2, further comprising, prior to said procuring, creating the signature counter as an attribute of the signature key.
4. The method in accordance with Claim 1 wherein the receiving input information comprises procuring the identifying characteristic to identify the signature device from said signature device.
5. The method in accordance with Claim 1, wherein the receiving input information comprises procuring information as to the hardware and software environment used in creating the digital signature.

6. The method in accordance with Claim 1, further comprising entering an identifying characteristic to identify a holder of the signature key prior to said receiving input information.
7. The method in accordance with Claim 6, further comprising creating the identifying characteristic to identify the holder of the signature key as an attribute of the signature key.
8. The method in accordance with Claim 7, further comprising changing the identifying characteristic to identify the holder of the signature key prior to said receiving.
9. An electronic signature device for generating a digital signature to sign a document comprising:
 - a) a receiver for receiving input information;

b) at least one storage location for storing at least a signature program and a certificate with signature key;

c) a data processor component for executing said signature program comprising at least a component for creating a signature data set comprising at least the received information, an identifier to identify said signature device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature, and a document extract value of the document for signing; and

d) an encryption component for creating an expanded digital signature by encrypting the signature data set with the aid of a signature key stored at said signature device.

10. The signature device in accordance with Claim 9, wherein the device is a chipcard.

11. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for generating a digital signature to sign a document in a signature device having a signature program and certificate with signature key stored thereon, said method steps comprising:

a) receiving input information to said signature device; and

b) executing said signature program by the steps of: creating a signature data set comprising at least the received information, an identifier to identify said signature device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature, and a document extract value of the document for signing; and creating an expanded digital signature by encrypting the signature data set with the aid of a signature key stored in said certificate.

13. The method in accordance with Claim 1, wherein said at least one identifying characteristic comprises information which uniquely identifies said digital signature in relation to every other digital signature generated with the same signature key.

IX. EVIDENCE APPENDIX

There is no additional evidence submitted pursuant to 37 CFR 1.130, 37 CFR 1.131 or 37 CFR 1.132.

X. RELATED PROCEEDINGS APPENDIX

There have not been any decisions rendered in any related proceedings.